INFOSEC-00002

**NSTISSI No. 4013**
**August 1997**

# NATIONAL TRAINING STANDARD FOR SYSTEM ADMINISTRATORS IN INFORMATION SYSTEMS SECURITY (INFOSEC)

**THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY**

# Form SF298 Citation Data

| | | |
|---|---|---|
| **Report Date**<br>*("DD MON YYYY")*<br>01081997 | **Report Type**<br>N/A | **Dates Covered (from... to)**<br>*("DD MON YYYY")* |

| | |
|---|---|
| **Title and Subtitle**<br>National Training Standard for System Administrators in Information Systems Security (INFOSEC) | **Contract or Grant Number** |
| | **Program Element Number** |
| **Authors** | **Project Number** |
| | **Task Number** |
| | **Work Unit Number** |
| **Performing Organization Name(s) and Address(es)**<br>National Security Agency NSTISSC Secretariat ATTN: V503 STE 6716 Fort George G. Meade, MD 20755-6716 | **Performing Organization Number(s)** |
| **Sponsoring/Monitoring Agency Name(s) and Address(es)** | **Monitoring Agency Acronym** |
| | **Monitoring Agency Report Number(s)** |
| **Distribution/Availability Statement**<br>Approved for public release, distribution unlimited | |
| **Supplementary Notes** | |
| **Abstract** | |
| **Subject Terms** | |
| **Document Classification**<br>unclassified | **Classification of SF298**<br>unclassified |
| **Classification of Abstract**<br>unclassified | **Limitation of Abstract**<br>unlimited |
| **Number of Pages**<br>36 | |

|  |  |
|---|---|
| **REPORT DOCUMENTATION PAGE** | *Form Approved*<br>*OMB No. 074-0188* |

|  |  |  |
|---|---|---|
| **1. AGENCY USE ONLY (Leave blank)** | **2. REPORT DATE**<br>8/1/97 | **3. REPORT TYPE AND DATES COVERED**<br>Guideline |

**4. TITLE AND SUBTITLE**

National Training Standard for System Administrators in Information Security Systems

**5. FUNDING NUMBERS**

**6. AUTHOR(S)**

National Security Agency

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**

|  |  |
|---|---|
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** | **12b. DISTRIBUTION CODE**<br>A |

**13. ABSTRACT** ***(Maximum 200 Words)***

This document published by National Security Telecommunications And Information Systems Security Committee, NATIONAL MANAGER. This instruction establishes the minimum course content or standard for the development and implementation of training for system administrator professionals in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

|  |  |
|---|---|
| **14. SUBJECT TERMS**<br>Infosec, information security, telecommunications security, | **15. NUMBER OF PAGES** |
|  | **16. PRICE CODE** |

|  |  |  |  |
|---|---|---|---|
| **17. SECURITY CLASSIFICATION OF REPORT** | **18. SECURITY CLASSIFICATION OF THIS PAGE** | **19. SECURITY CLASSIFICATION OF ABSTRACT** | **20. LIMITATION OF ABSTRACT** |
| Unclassified | UNCLASSIFIED | UNCLASSIFIED | None |

National Security Telecommunications And Information Systems Security Committee

## NATIONAL MANAGER

## FOREWORD

1. This instruction establishes the minimum course content or standard for the development and implementation of training for system administrator professionals in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

NATIONAL SECURITY AGENCY
NSTISSC SECRETARIAT
ATTN: V503 STE 6716
Fort GEORGE G. MEADE, MD 20755-6716

KENNETH A. MINIHAN
Lieutenant General, USAF

# NATIONAL TRAINING STANDARD
# FOR
# SYSTEM ADMINISTRATORS
# IN
# INFORMATION SYSTEMS SECURITY (INFOSEC)

SECTION
PURPOSE .......................................... .
APPLICABILITY. ......................................... II
RESPONSIBILITIES ..................................... III

## SECTION I - PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of training for System Administrators in the disciplines of telecommunications and information systems (IS) security.

## SECTION II - APPLICABILITY

2. National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 establishes the requirement for federal departments and agencies to implement training programs for INFOSEC professionals. As defined in NSTISSD 501, an INFOSEC professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. That directive is being implemented in a synergistic environment among departments and agencies which are committed to satisfying these INFOSEC education and training requirements in the most effective and efficient manner possible. This instruction is the continuation of a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (NSTISSI Nos. 4011, 4012, 4013, and 4014). The definitions for words used in this instruction are derived from the National INFOSEC Glossary, NSTISSI No. 4009. The references pertinent to this instruction are listed in ANNEX B. Other documents which can be used in conjunction with this document are listed in ANNEX C.

3. The body of knowledge listed in this instruction may be obtained from a variety of sources, i.e., the National Cryptologic School, the General Services Administration (Office of Information Security), and Government contractors, as well as from adaptations of existing department/agency training programs, or from a combination of experience and formal training. ANNEX A lists the minimal INFOSEC performance standard for an SA.

4. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of training for System Administrators in the disciplines of telecommunications and IS security.

## SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that System Administrators (or their equivalents) are made aware of the body of knowledge outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6. The National Manager shall:

a. maintain and provide an INFOSEC training standard for System Administrators to U.S. Government departments and agencies:

b. ensure that appropriate INFOSEC training courses for System Administrators are developed: and

c. assist other U.S. Government departments and agencies in developing and/or conducting INFOSEC training activities for System Administrators as requested.

## ANNEX A

## MINIMAL INFOSEC PERFORMANCE STANDARD FOR SYSTEM ADMINISTRATORS

### Job functions

The INFOSEC functions of a System Administrator are:

(1) working closely with the Information Systems Security Officer (ISSO) to ensure the Information System or network is used securely;
(2) participating in the Information Systems Security incident reporting program;
(3) assisting the ISSO in maintaining configuration control of the systems and applications software;
(4) advisingthe ISSO of security anomalies or integrity loopholes; and
(5) administering, when applicable, user identification or authentication mechanism(s) of the IS or network.

### Terminal Objective:

Given various simulated scenarios and typical situations containing information systems security issues, the System Administrator will be able to describe and apply the appropriate actions to manage and administer the IS(s) in a secure manner. To be acceptable, the description must be in accordance with applicable INFOSEC regulations, policies, and guidelines.

### List of performance items under competencies

In each of the competency areas listed below, the System Administrator shall perform the following functions:

1. GENERAL

a. Security Policy

(1) define local accountability policies;
(2) explain accreditation;
(3) discuss three agency specific security policies:
(4) define assurance;
(5) explain certification policies as related to local requirements;
(6) define local e-mail privacy policies:
(7) describe local security policies relative to electronic records management;
(8) explain security policies relating to ethics;
(9) describe relevant FAX security policies;
(10) discuss the concept of information confidentiality;
(11) identify information ownership of data held under his/her cognizance:
(12) identify information resource owner/custodian;
(13) define local information security policy;
(14) describe information sensitivity in relation to local policies;
(15) discuss integrity concepts:
(16) describe local policies relevant to Internet security;
(17) explain local area network (LAN) security as related to local policies;
(18) define policies relating to marking of sensitive information;
(19) understands fundamental concepts of multilevel security:
(20) describe policies relevant to network security;

(2 1) define the functional requirements for operating system integrity;
(22) perform operations security (OPSEC) in conformance with local policies;
(23) explain physical security policies;
(24) discuss local policies relating to secure systems operations;
(25) identify appropriate security architecture for use in assigned IS(s);
(26) describe security domains as applicable to local policies;
(27) define local policies relating to separation of duties;
(28) identify systems security standards policies;
(29) identify DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), or Orange Book policies:
(30) identify TEMPEST policies:
(3 1) define TEMPEST policies;
(32) define validation and testing policies;
(33) identify verification and validation process policies;
(34) define verification and validation process policies;
(35) describe wide area network (WAN) security policies;
(36) use/implement WAN security policies:
(37) describe workstation security policies;
(38) use/implement workstation security policies; and
(39) describe zoning and zone of control policies.

b. Procedures

(1) practice/use facility management procedures;
(2) describe FAX security procedures;
(3) practice/use FAX security procedures;
(4) describe housekeeping procedures;
(5) perform housekeeping procedures;
(6) describe information states procedures;
(7) distinguish among information states procedures;
(8) explain Internet security procedures;
(9) use Internet security procedures;
(10) explain marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms, March 30, 1987);
(11) perform marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms, March 30, 1987);
(12) apply multilevel security:
(13) explain the principles of network security procedures;
(14) use network security procedures;
(15) describe operating system integrity procedures;
(16) perform operating systems security procedures;
(17) assist in local security procedures:
(18) describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI), or Red Book:
(19) describes secure systems operations procedures;
(20) define TEMPEST procedures;
(21) identify TEMPEST procedures;
(22) identify certified TEMPEST technical authority (CTTA);
(23) describe WAN security procedures;
(24) practice WAN security procedures; and
(25) explain zoning and zone of control procedures.

c. Education, Training, and Awareness

(1) discuss the principle elements of security training;
(2) explain security training procedures;
(3) explain threat in its application to education, training, and awareness;
(4) use awareness materials as part of job;
(5) distinguish between education, training, and awareness;
(6) give examples of security awareness;
(7) give examples of security education;
(8) discuss the objectives of security inspections/reviews; and
(9) identify different types of vulnerabilities.

d. Countermeasures/Safeguards

(1) discuss the different levels of countermeasures/safeguards assurance;
(2) describe e-mail privacy countermeasures/safeguards;
(3) define Internet security:
(4) describe what is meant by countermeasures/safeguards;
(5) describe separation of duties;
(6) define countermeasures/safeguards used to prevent software piracy;
(7) define TEMPEST countermeasures/safeguards; and
(8) explain what is meant by zoning and zone of control.

e. Risk Management

(1) explain ways to provide protection for Internet connections;
(2) describe operating system integrity;
(3) define TEMPEST as it relates to the risk management process:
(4) identify different types of threat;
(5) explain WAN security; and
(6) explain what zoning and zone of control ratings are based on.

2. ACCESS CONTROL

a. Policies/Administration

(1) use network access controls as designed;
(2) explain compartmented/partitioned mode;
(3) describe data access:
(4) identify the dedicated mode of operation:
(5) explain electronic records management;
(6) define information ownership;
(7) identify information resource owner/custodian;
(8) describe separation of duties; and
(9) define the system high mode.

b. Countermeasures

(1) describe use of caller ID;
(2) give five examples of countermeasures;
(3) define internal controls and security:
(4) identify methods of intrusion detection;
(5) define network firewalls; and
(6) describe network security software.

c. Safeguards

(1) demonstrate the ability to use alarms, signals, and reports:
(2) identify network security software;
(3) describe operating system security features;
(4) define protected distribution systems; and
(5) describe system security safeguards.

d. Mechanisms

(1) discuss authentication mechanisms;
(2) describe discretionary access controls;
(3) describe mandatory access controls;
(4) describe one-time passwords;
(5) discuss privileges; and
(6) define single sign-on.

3. ADMINISTRATIVE

a. Policies/Procedures

(1) identify basic/generic management issues:
(2) define change control policies;
(3) discuss documentation:
(4) explain electronic records management;
(5) describe object reuse:
(6) define operational procedure review;
(7) discuss policy enforcement;
(8) identify procedures;
(9) discuss security inspections; and
(10) describe local password management policy.

b. Countermeasures/Safeguards

(1) give examples of alarms, signals and reports;
(2) define application development control:
(3) assist in preparing assessments:
(4) identify countermeasures:
(5) describe disaster recovery procedures:
(6) discuss disposition of classified information;
(7) practice disposition of media and data;
(8) practice document labeling;
(9) discuss proper use of security safeguards;
(10) define separation of duties;
(11) identify storage media protection and control; and
(12) define system software controls.

4. AUDIT

a. Policies/Procedures

(1) use alarms, signals and reports in accordance with existing policies and procedures;
(2) summarize audit-related documentation;
(3) discuss electronic records management relative to compliance with local policies and procedures; and
(4) describe three policies and/or procedures in which separation of duties is appropriate or mandatory.

b. Countermeasures/Safeguards

(1) identify two countermeasures applicable to audit trail tampering; and
(2) describe three safeguards gained through use of audit trails.

c. Tools

(1) explain two major benefits of auditing;
(2) identify three audit tools;
(3) describe the major benefit gained through use of audit trails and logging policies:
(4) define an error log;
(5) explain two capabilities offered by expert security/audit tools;
(6) identify two intrusion detection systems; and
(7) describe the major operating system security features.

5. OPERATIONS

a. Policies/Procedures

(1) describe disaster recovery policies and procedures:
(2) use/implement disaster recovery policies and procedures;
(3) define disaster recovery policies and procedures;
(4) describe documentation policy and procedures:
(5) use/implement documentation policy and procedures:
(6) discuss object reuse policy and procedures;
(7) describe separation of duties policies and procedures:
(8) practice/implement separation of duties policies and procedures;
(9) identify disposition of media and data policies and procedures;
(10) perform disposition of media and data policies and procedures;
(11) explain disposition of media and data policies and procedures; and
(12) identify storage media protection/control policies and procedures.

b. Countermeasures/Safeguard

(1) use countermeasure/safeguard alarms, signals and reports;
(2) describe countermeasures:
(3) use/implement countermeasures/safeguards;
(4) discuss countermeasure/safeguard corrective actions;
(5) assist in performing countermeasure/safeguard corrective actions;
(6) describe safeguards; and
(7) use/implement safeguards.

c. Management/Oversight

(1) use/implement management/oversight change controls;
(2) describe configuration management;

(3) discuss database integrity;
(4) describe disaster recovery management/oversight:
(5) use/implement disaster recovery management/oversight;
(6) discuss electronic records management/oversight;
(7) identify the key elements of information integrity;
(8) discuss information management;
(9) explain risk management; and
(10) practice risk management.

6. CONTINGENCY

a. Continuity of Operations

(1) practice backups:
(2) describe continuity planning:
(3) describe disaster recovery:
(4) describe disaster recovery plan testing: and
(5) discuss disaster recovery planning.

b. Countermeasures/Safeguards

(1) use alarms, signals and reports;
(2) define information availability;
(3) identify examples of corrective actions:
(4) select countermeasures;
(5) identify methods of intrusion detection; and
(6) select appropriate safeguards.

c. Configuration Management

(1) practice change controls;
(2) explain database integrity:
(3) practice disposition of classified info;
(4) perform disposition of media and data;
(5) perform electronic records management:
(6) practice emergency destruction; and
(7) identify storage media protection and control procedures.

7. PLATFORM SPECIFIC SECURITY FEATURES/PROCEDURES

To be determined by agency/service/organization ISSO.

# ANNEX B

# REFERENCES

The following references pertain to this Instruction:

a. NSTISSD 50 1, National Training Program for Information Systems Security (INFOSEC) Professionals, dated 16 November 1992

b. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated June 5, 1992

c. DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985

d. C.F.R. 32 Section 2003, National Security Information - Standard Forms, dated March 30, 1987

## ANNEX C

## BIBLIOGRAPHY

1. P.L. 100-235, Computer Security Act of 1987, dated January 8, 1988

2. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990

3. OMB Circular A- 130, Appendix III, Security of Federal Automated Information Systems, dated February 8, 1996

4. Office of Personnel Management, 5 CFR Part 930, Training Requirements for the Computer Security Act, dated January 3, 1992

5. National Computer Security Center TG-005, Trusted Network Interpretation (TNI), dated July 3 1, 1987

- All listed above except Power Users.
- Server Operators - can manage domain servers.
- Account Operators - can manage user accounts and groups.
- Print Operators - can manage printers.
- Replicator - supports file replication.

### Global Groups

Global groups maintained on a Windows NT domain may have domain user accounts as members, and are used to administer domain users. System administrators can effectively use global groups to sort users based on their needs. This can be accomplished by placing the global group in the appropriate local groups, assigning the users permissions and granting them the rights they need to perform their jobs. As mentioned, global groups can only have domain user accounts as members. No other groups can be members of a global group. This is due to the fact that the system administrator assigns permissions and grant rights to the local groups (because the local system or domain server holds the resources) and then makes the global groups members of the local groups.

Windows NT provides two built-in global groups each with established permissions and rights. They are:

- Domain Admins - contains the domain administrator account by default and is a member of the domain level Administrators local group and the system level Administrators local group for Workstations in the domain.
- Domain Users - contains all the domain users.

### Special Groups

Special groups are created by Windows NT for unique or specific purposes and can not be viewed, changed, or have members added to them in the User Manager. A users membership to a special group is determined by how they access resources on the system. Special groups may be assigned access permissions in some cases and may be seen when a system administrator is assigning permissions on Windows NT objects.

The following is a list special groups and a description of their membership:

- Network - any user connected to a system via the network.
- Interactive - any user logged on interactively at a local system
- Everyone - any user logged on to the system (both the Network and Interactive groups).
- Creator Owner - the user that created or took ownership of an object.

- System - the Windows NT operating system.

***Note*** If the user were the system administrator or other user that is a member of the Administrators group, the Administrator group would be a member of the Creator Owner group.

The special group that system administrators must pay close attention to is the **Everyone group.** As stated above, all users logged on are members of this group. Therefore, any access permissions assigned to the Everyone group allowing or denying access to objects is by default assigned to all users.

For example, if a file should only be accessed by a certain group, the system administrator could not assign permissions to that group allowing file access and then assign permissions to the Everyone group denying file access. Since Windows NT acts on all deny ACEs before allow ACEs, it would stop when it found the deny ACE for the Everyone group and no one would be allowed access including the group with permissions assigned to allow access to the file.

***Access Control*** Each file and directory object has an Access Control List (ACL) that contains a list of Access Control Entries (ACEs). ACEs provide information regarding access or auditing permissions to the object for a user or group of users. Along with the file system, they protect objects from unauthorized access.

There are three different types of ACEs:

- System Audit
- Access Allowed
- Access Denied

System Audit is a system ACE used for logging security events and audit messages. Access Allowed and Access Denied are known as discretionary ACEs. They are prioritized by the type of access: Denied and Granted. Deny always overrides grant access. If a user belongs to a group with Access Denied privileges to an object, the user will be denied access regardless of any granted access he possesses from his own user account, or in other groups to which he is included.

Discretionary ACLs allow owners to control the access of their objects. Controls over objects can be applied to individual users, multiple users, and groups. They can be set by the object's owner, a user who has an administrator account, or any user with correct permissions to control resources on the system. If a discretionary ACL is not specified for an object, a default ACL is created. Default ACL file objects inherit access controls from their parent directories.

***Warning*** Be sure to evaluate your object's ACLs after installing Windows NT. Most versions are shipped with file ACLs set to give Everyone Full Control access.

### User Rights

User authorization to perform specified actions on a system is called rights. Rights apply to the entire system. They are usually assigned to groups or users by the system administrator. Rights give users access to services such as backing up files and directories, shutting down the computer, logging on interactively or changing system times, that normal discretionary access controls do not provide.

Due to NT's modular approach of file system management, multiple file systems are supported. NT uses low-level drivers as a part of the NT Executive to support each file system. This provides the ability to expand to additional file systems as they are introduced by simply installing a new driver.

NT 4.0 supports two file systems: NTFS and FAT.

### FAT File System

The File Allocation Table (FAT) file system is named after it's organizational method. The FAT file system was originally designed for small disks and simple directory structures. Its design has since evolved to support larger disks and more powerful systems. It is most widely used for systems that run the DOS operating system.

The FAT file system doesn't support the security features or the automatic disk restoration utilities that NT provides. Using the FAT file system is not recommended for volumes shared across the network. The following configurations do require the FAT file system structure:

- Dual-boot system configurations with DOS or OS/2 volumes.
- FAT is the only file system available for formatting diskettes on Windows NT.
- RISC-based systems must provide a FAT partition to boot system files. NT provides a tool to secure the FAT system partition on this type of system.

**✓ Tip** If there is no need to boot DOS, and the system is not an RISC architecture, using FAT file systems are not recommended. 1

### NTFS File Systems

NTFS was developed to support the Windows NT file and directory security features. It is the only file system available on NT that provides the capability to assign permissions to individual files. The NTFS driver that allows access to an NTFS volume is loaded in NT so unauthorized users cannot access NTFS volumes by booting the system from a DOS diskette.

NTFS also prevents users from undeleting files or directories that have been removed from NTFS volumes. Since NT doesn't give undeleted programs access to work on an NTFS volume, even files that still exist on the disk are not available. NTFS provides file system recovery where disk activities can be logged to enabling activities to be restored in the case of a system crash. Chances of corrupting data, due to power or hardware failures, are small with NTFS.

### Physical Security and NTFS

NTFS file system security is only valid if the ability to access the system from DOS, or another operating system is eliminated. The following precautions for physical security should be examined:

- Remove or lock floppy drives.
- Require boot passwords on servers and set the BIOS to disable booting from a floppy drive. In most cases, removing the battery disables the BIOS lock.
- Do not create any DOS partition on the server.
- Lock the system in a secure location.
- Set alarms alerting you to when a server is shut down, so an intruder can be caught during a potential attack.

**Warning** A program called **ntfsdos.exe** is available to read files protected by Windows NTFS. The program is run after booting a system with a DOS diskette. This is not a security risk if the proper physical security measures are taken or floppy drives are not available on the system.

### NTFS vs. FAT

- NTFS provides extended security features not available with the FAT file system.
- NTFS is built for speed. It uses a binary tree structure for directories to reduce the access time needed to locate files.
- NTFS minimizes file fragmentation in large disk volumes.
- NTFS uses small cluster sizes (512 bytes) to prevent wasted disk space.
- NTFS provides the ability to selectively compress individual files and directories or actual volumes on disks.

### Shares

The Shared Directory feature in the File Manager allows sharing of files and directories over the network. Shared object permissions can be established for FAT or NTFS file structures. The user must be a member of the Administrator group or Server Operator group to work with shared directory permissions. Users are unable to access files on a system through the network until there is a shared directory available.

Once a directory has been shared on the system, users can log on to that system and be able to access the shared directory. To use the directory, the user must assign the share to an unassigned drive letter. When the directory is assigned a drive letter, the share can be accessed just like another hard disk on the system. Directory sharing can be viewed and stopped by an Administrator or Server Operator.

### Object Permissions

File and directory permissions are the foundation of most user-controlled security in Windows NT. Permissions are the rules associated with a particular object, which describe which users can access what objects, and how they have access to the objects. Object permissions for files are only available for files stored on NTFS volumes. File and directory permissions are cumulative, but the No Access permission overrides all other permissions.

The types of file access permissions are:

- No Access
- Read
- Change
- Full Control
- Special Access

For directory access the following permissions are added:

- List
- Add
- Read

### Object Ownership

Object ownership allows the user to change permissions on the owned object. The user who is the creator of a file or directory is usually the owner. Users can't give away ownership of their objects, but they can give other users permission to take ownership. This prevents users from creating objects and making them appear to be owned by another user.

Ownership of a file or directory can be taken by an Administrator without the owners consent, but the Administrator can't transfer ownership to others. Administrators cannot access private files without leaving some trails behind, because after claiming ownership, Administrators cannot return ownership to the original owner.

Monitoring is a continuous evaluation of system-level attributes that could reveal system compromise. Monitoring also provides reporting and follow-up mechanisms on attempted violations to the system. Auditing systems validates compliance when using monitoring procedures. In addition, auditing is used in follow-up actions.

There are two types of security monitoring: status and event monitoring. Status monitoring involves current states or processes of the system. Event monitoring evaluates audit trails, which occurs after processes have finished running. Auditing is provided to evaluate the control structure, assess risk, determine compliance, report on exceptions and make improvements to the system. Systems should be evaluated against the organization's security policies and compliant technical platforms to the security implementation standards.

The monitoring section of a site security plan should include:

- Systems and subsystems to audit
- Tools and configuration settings
- Schedules for periodic auditing tasks
- Review and testing of audit coverage and functionality

In order to obtain a secure system environment, effective information security requires physical, administrative and operational policies combined with solid security and auditing features. Together, these components can protect systems against malicious or accidental access, damage to, or loss of data.

### DOE Computer Security Orders

There are two DOE Computer Security Orders: The Unclassified Computer Security Program DOE 1360.2B, and the Classified Computer Security Program DOE 5639-6A-1.

### NIST Recommendations

Ensuring your organization controls and monitors the security of your systems can be achieved by implementing security policies and procedures that employees can follow. It is critical to document the policies in a site security plan. This plan should be reviewed periodically since networks and resources change rapidly. A small change can open up a site to a larger or completely new risk.

- The National Institute for Standards and Technology (NIST) has defined the following security standards which are called the Minimal Security Functional Requirements for Multi-User Operational Systems. These standards can be used as a baseline for developing your own security policies and procedures:

- Identification and authentication: identifying and validating users through the logon process, and authorization to use systems based on this validation.

- Access control: controlling users access to the network resources and files by setting rights and permissions.

- Accountability and auditing: tracking and logging activities linked to specified users on the network.

- Object reuse: providing multiple users access to individual resources.

- Accuracy: protecting resources from errors, corruption and intrusion.

- Reliability: systems and resources are available and protected against failure or loss.

- Data exchange: securing data transmission over the network.

### Department of Energy

User Warning Notice as defined by DOE classified order 5639.6A-1:

***WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties.***

### Department of Justice

Sample banner from the Department of Justice:

***This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel: In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.***

**Access Control Entry (ACE).** Entries in the ACL that provide information regarding access or auditing permissions to objects for users or groups.

**Access Control List (ACL).** A list connected to each object specifying various ACEs.

**Access Controls.** Limits that prevent users from having total access to information systems.

**Access token.** LSA checks the policy database and retrieves the user rights and other SID information to create the token.

**Account domain.** Another word for trusted domain.

**Backup Domain Controller (BDC)**. Hold a copy of the security database and user account information in the case of failure of the PDC.

C2 **level secure.** A level of security for systems defined by the National Computer Security Center (NCSC) of the United States Department of Defense in the trusted computer system evaluation criteria document.

**Discretionary access controls.** Allowed and denied access control entries in an objects access control list.

**Domain.** Collection of servers grouped together which share a security policy and a user account database.

**File Allocation Table (FAT).** File system structure.

**Hives.** Data located in the four registry subtrees derived from sets of files. The files are either data or log files.

**Keys.** Value entries contained in the subtrees of the NT registry.

**Local Security Authority (LSA).** Heart of security subsystem, which validates local and remote logons to all types of accounts.

**Logon authentication.** Windows NT logon process that verifies user information and authenticates user.

**Master domain.** Domain configuration consisting of multiple domains and one main master domain.

**NT Executive.** Provides a set of common services that all environment subsystems can use.

**NT File System (NTFS).** Windows NT file system structure.

**NT Security Model.** The foundation of security in the Windows NT OS.

**NT sewer.** Software that provides NT OS including extended networking features.

**NT workstation.** Same piece of software as NT server except is limited to ten simultaneous network connections.

**Object ownership.** Usually the creator of the object.

**Objects.** Representation of files, directories, memory, devices, system processes, or threads in the NT operating system.

**Permissions.** Rules associated with an object describing which access users have.

**Primary Domain Controller (PDC).** Server in a domain that maintains the security and user account databases for that domain.

**Registry.** Database that contains applications, hardware, device driver configuration data, network protocols, and adapter card settings.

**Resource domain.** Another word for trusting domain.

**Rights. See** user rights.

**SAM database.** Contains all user and group account information. It is part of the security subsystem which provides user validation services.

**Security identifier (SID).** A unique ID associated with each user account.

**Security policy and procedures.** An organization's statement about how it will provide security, handle intrusions, and recover from damage caused by security breaches.

**Security policy for domains.** Consists of password policies and account lockout policies.

**Security Reference Monitor (SRM).** Part of security subsystem responsible for enforcement of access validation and audit generation policies required by the LSA.

**Security Subsystem.** The combination of the logon processes, LSA, SAM, and SRM in the NT security model.

**Sewer.** The piece of hardware in a client/server environment that holds software and hardware shared among its clients.

**Shares.** Sharing of files and directories over the network.

**Subject.** The user's access token connected with each process the user runs.

**Trusted domain.** Makes accounts available for use in the trusting domain.

**Trusting domain.** Contains the resources the trusted domain will access.

**Trusts.** An administrative way to link together two domains allowing one domain's users access to the other domain.

**User account database.** Holds account information for all users that can log into a domain.

**User authentication.** Determined by validation of the SAM database to the user logon information.

**User rights.** Authorization to perform specified actions on a system.

**Workgroup.** A single system or multiple systems that are not connected to a domain.

http://csrc.ncsl.nist.gov/nistbul/csl96-05.txt

THE WORLD WIDE WEB: MANAGING SECURITY RISKS
> Computer users are finding the Internet and the World Wide Web
> (or Web for short) extremely useful for browsing through
> information, publishing documents, and exchanging information.
> Web applications have become popular because of the availability
> of powerful personal computers (PCs) capable of high quality
> graphics, easy Internet access, and a simple hypertext markup
> language (HTML) and network protocol.

> As a result, many organizations and individuals are becoming
> Web-aware. The Web offers all kinds of information, from
> research papers, to customer support and marketing information,
> to club calendars and family bulletin boards. A myriad of Web
> indexing and searching services allow readers to find what
> they're looking for. Organizations also use Internet protocols
> to support their internal networks (often called intranets).

> Although the Web is used for other applications such as
> electronic commerce, the primary one is Internet publishing.
> This CSL Bulletin addresses general security issues related to
> the use of the World Wide Web, concentrating on risk management
> for Web readers and publishers.
>
> A Web reader is anyone who uses a Web browser (a Web client
> application which typically supports more than one Web protocol)
> for access to Web-based information. A Web publisher is a person
> or organization that uses a Web server to provide information and
> access to applications for internal or external users.
>
> Note: Any mention of particular technologies or commercial
> products is for the purposes of explanation and illustration
> only. It does not imply a recommendation or endorsement by NIST
> or the U.S. Department of Commerce.
>
> WEB READERS
> The goal of risk management is to balance expected gains against
> unexpected losses, so as to maximize overall gain and minimize
> loss. Some readers may be using the Web just for fun, but
> organizational users have more to lose (and gain). Some of the
> gains a Web reader might expect are:

> - a more user-friendly interface;

> - more timely access to information;

> - access to more or previously unavailable information; and

> - keeping current with technology.

> Quantifying those gains can be difficult. One measure would be
> an estimate of how much more time would have been spent getting
> the information via other means. Potential losses are somewhat
> easier to quantify.

> Losses
> Some of the more likely losses and their causes that a Web reader
> faces are:

> Damage to the system and user information from buggy software,

> virus-infected executables, trojan horse programs, embedded macros, and downloadable applets (an applet is a small program that is downloaded and executed on-the-fly by the browser). Some recent viruses can even erase the boot EPROMs (Erasable Programmable Read Only Memory) of some PCs, rendering them unusable.
>
> Monetary or credit damage from illegitimate companies or Web-based scams, or by having credit card information stolen via network sniffing or break-ins at the server.
>
> Privacy can be compromised when information regarding a user's browsing activities is published or sold. The reader's Internet address, date and time, and the names of the files accessed may be recorded by the Web server. If the Web reader fills out any form, additional information may be recorded as well.
>
> Reputation can be damaged by individuals who expose information about the reader, or who masquerade as the reader and perform antisocial acts. For example, a Web applet could cause the Web reader's browser to send email of the applet author's choice.
>
> Most threats that the Web reader faces are not new, but the Web makes them potentially more hazardous. For example, viruses have been around for years, but the point-and-click Web browser interface makes it easy to instantly download and execute an infected program. Anyone with a telephone is exposed to telemarketing scams, but a virtual Web storefront with fancy graphics somehow seems more trustworthy than a stranger's voice over the telephone. Many companies collect and sell customer purchase information, but one wouldn't expect the act of reading an online brochure to add one's email address to a telemarketing database.
>
> Threats
>
> Web threats stem from shortcuts in the software development process, shortcomings in popular operating systems, deficiencies in the Internet protocols, and the problems inherent in managing the Internet.
>
> Buggy software is endemic to the software development process. Developers continually add new features to differentiate their products and increase market share. Users usually prefer to use the latest and greatest version of any new Web client or server. Much of the software is provided on a try-before-you-buy basis, which allows people to test-drive software but provides no warranty in the event of bugs.
>
> Web browsers are especially hazardous because they can allow access to untrustworthy systems on the Internet and they often invoke other applications as a side effect of their use. Some may also act as an FTP (file transfer protocol) client, Usenet news (Internet-based discussion groups) client, or an email client. Each new feature increases the risk of a dangerous bug.
>
> Impersonation of an individual or organization is difficult to prevent on the Internet. Computer user identification is usually meaningful only within an organization and depends on the policies within that organization and how well they are enforced. An email address may or may not uniquely identify an individual, and many organizations do not provide outside access to internal

> email addresses. In any case, email is usually easy to forge, being the electronic equivalent to a postcard written in pencil. Although secure email protocols have been proposed, none has been widely implemented.
>
> When a browser connects to a Web server, the server gets the Internet address of the connecting system. If it is a multi-user system, the server cannot tell what user on the system connected. The address of a single-user PC may not be very useful either, since systems using dial-up TCP/IP (Transmission Control Protocol/Internet Protocol) may be assigned a different address every time they connect.

> Until recently, the agency responsible for registering most Internet Domain names only confirmed that the requested name was unique. It did not require proof that a name like ORPHANS.ORG was going to be used by a nonprofit organization or that WXY.COM was an actual business entity. Consequently, an Internet user has no dependable way of identifying and authenticating an individual or organization on the Internet.

> Eavesdropping (also known as sniffing or snooping) of network traffic is unavoidable as long as local area networks (LANs) use broadcast protocols and the data are unencrypted and travel over public networks. You should be at least as cautious using the Web for sensitive matters as you would be discussing something confidential on a public or cellular telephone.

> The costs associated with recovering from losses can be minor or major. Users can spend days recovering from a virus infection. Data corruption is more difficult to discover and recover from, since there may be no obvious symptoms. Impersonation could result in anything from a forged love letter to an order for 10,000 pizzas (with anchovies).
>
> ### Risk Control
> Some remedies exist to reduce some of the risks to a Web reader. The easiest to implement are those based on loss avoidance.

> - If you don't use the Web, you're not exposed to its dangers.
>
> - If you never download executable code, your system won't be infected by a virus.

> - If you don't buy things over the Web, you can't be cheated.

> - If you never give out financial information (like credit card numbers or bank account numbers) over the Web, it can't be misused or stolen.

> Other remedies are based on loss control or mitigation.

> - Backup your system regularly. Be sure that you can recover your software and data in the event of a crash or virus infestation.
>
> - Be a careful shopper to reduce the danger of buggy software. Buy from known sources. Don't run beta test code. Buy the simplest browser that gets the job done. Turn off features you don't use. Don't download every viewer and applet you run across.

>
> - If your organization has one, test new Web applications on a
>   sacrificial computer system that is isolated from the
>   internal network and doesn't contain any important data.

> - Until better security mechanisms are in widespread use, if
>   you must buy over the Internet, take some precautions.
>   Check the identity of the vendor via another channel, e.g.,
>   paper mail or telephone listing. Patronize vendors that use
>   a Web server with a secure channel between your system and
>   theirs.

> Impersonation
> The problem of impersonation is somewhat difficult to solve. An
> organization can maintain tight controls over the hardware and
> software of its intranet to make impersonating someone else
> within the organization relatively difficult. It can also
> usually exercise some form of discipline over its members to
> prevent or punish transgressions. The greater Web is part of the
> Internet, which is an international system of networks. No one
> has authority to prevent or punish abuses across the entire
> Internet.

> A form of public key encryption can be used to identify
> individuals, computer systems, and organizations. As yet, there
> is no global infrastructure to support the management of the
> keys. Individual organizations can still choose to implement
> this kind of identification for their intranet, and some
> commercial Web servers and browsers implement a vendor-specific
> form of key exchange so that Web servers can authenticate
> themselves to browsers.
>
> Eavesdropping
> >From a technical perspective, the simplest remedy for
> eavesdropping is to encrypt messages and channels. However, the
> use of encryption for confidentiality has the same drawbacks
> associated with using encryption for personal identification. It
> is relatively easy to implement within an organization, but hard
> to implement between organizations. Encryption of all network
> traffic can be expensive in terms of hardware, software, and
> central processing unit (CPU) cycles.
>
> Several commercial Web servers and browsers support encryption of
> all Web requests between the browser and server. Currently, most
> secure servers can only talk to browsers from the same vendor and
> can only use keys from a limited set of key certificate
> authorities. Eventually, most Web vendors will be using Web
> servers that provide public key-based authentication of the
> server and encryption of the channel between the browser and
> server.

> Organizational Support for Readers
> Organizations need to provide guidance and support to their Web
> readers. An organization should have clear, workable, and
> enforceable Web usage and security policies.

> Some measures an organization can take are:

> - Buy licensed software from a trusted vendor;

> - Run proactive virus checkers;

> - Distribute approved browser configuration files and trusted viewers; and
>
> - Educate your readers. Tell them:
>
>   what's allowable usage, covering issues like private email, Usenet posting, personal browsing, etc.;
>
>   not to download unapproved browsers, viewers, and applets; and
>
>   not to configure their Web browser to automatically invoke an application just because the Web server suggests it.
>
> Particular technologies such as active forms or downloadable applets must be carefully examined and approved before being approved for organizational use.
>
> WEB PUBLISHERS
>
> Web publishers face the same challenges as Web readers. They need to recognize the potential losses from various threats and implement risk reduction measures.
>
> Losses
>
> The types of losses a Web publisher can incur are similar to those of a Web reader, namely:
>
> Damage to their systems and networks from buggy and misconfigured server software, insecure Common Gateway Interface (CGI) programs, and untrustworthy server-side applets.
>
> Monetary and credit damage by theft of service, nonpayment, credit card fraud, etc.
>
> Privacy can be compromised when the organization's or its customers' confidential information is exposed.
>
> Reputation can be damaged if information is changed or lost, confidential customer information is exposed, or service is denied.
>
> Threats
>
> Buggy or misconfigured Web server software can damage or allow damage to information or software. Security-related bugs have been discovered in all of the popular UNIX-based Web servers. Most of the bugs were caused by chronic UNIX/C errors in string handling, environment variables, and the use of the system() call. Theoretically, since the source code was available for most of the servers, the errors should have been immediately spotted by the Internet users who downloaded the code. Practically, however, most users download a binary executable and never look at the source code, or merely give it a cursory look before compiling and installing it. Users assume that someone more conscientious than themselves has carefully studied the code.
>
> Most Web servers provide some kind of access control; they can be configured to accept or deny connections based on Internet address or domain name. There are several problems with this

> method.  As described above, Internet addresses and domain names
> are a weak identification method.  Also, unless you can configure
> an attack computer with various addresses, it is difficult to
> tell if your configuration rules are correct or if the Web server
> author implemented the access control algorithms correctly.

> Web servers support dozens of optional features.  The most
> popular features are usually the best debugged, since other
> people have already discovered the problems.  If you use
> little-used or experimental features, you are the guinea pig.
>
> CGI programs allow the Web server to execute an external program
> when particular URLs (Uniform Resource Locators) are accessed.
> This provides a gateway to other programs that may query a
> database or create on-the-fly HTML.  Unfortunately, it's easy to
> create insecure CGI programs that allow an attacker to trick the
> Web server into executing other programs.  Only careful
> configuration of the Web server and CGI program, and careful
> review of the CGI code, can prevent those mistakes.

> If the Web server is broken into, it can serve as a stepping
> stone to break into other networks and systems in the
> organization.  The privacy of the organization and its customers
> can be violated if confidential data are kept on the Web server.
> Production systems could be damaged or brought down. If
> financial data are kept on the Web server, they could be altered
> or stolen.  The reputation of the organization can be damaged if
> information is maliciously altered or customers are denied
> service.

> Risk Control
> Exercise central coordination of Web publishing in your
> organization.  Establish procedures for verifying the security
> and integrity of your Web servers and their contents.

> Keep it simple.  Run the Web server on a stripped-down system,
> i.e., turn off nonessential network protocols, create the minimum
> necessary user accounts, and remove nonessential software.

> Partition your systems to limit the damage that can be done.  For
> example:

>   –  Don't put confidential data on a publicly accessible server.
>
>   –  Don't run a publicly accessible server on an internal
>      production system or on your internal network.

>   –  Store confidential customer data, like credit card
>      information, on a tightly controlled system, apart from the
>      Web documents.
>
>   –  If possible, store read-only data on immutable media.

>   –  Don't do program development on the server system.  Keep
>      compilers off the server.

>   –  Configure the network and internal systems such that the Web
>      server system is not trusted.

>   –  Don't allow that system access to internal resources, such
>      as network filesystems, printers, and accounts.

>
> Track Web software bug reports, especially security-related ones.
> Track developments in Web security, in the areas of encryption,
> authentication, and payment protocols.
>
> Tell Web software vendors that quality is more important than
> endless new features.
>
> SUMMARY
> You have to protect yourself, because all other controls are
> after the fact. The university may never discipline the student
> who broke into your system. The Federal Bureau of Investigation
> may never find the money you lost in an interstate Internet scam.
> You don't want to have to wait for Interpol to investigate your
> case.

> As the Internet and the World Wide Web evolve, you must continue
> to educate yourself and your organization as new protocols, file
> formats, applications, and products are introduced.

> For More Information

> WWW Consortium Security Resources

> http://www.w3.org/pub/WWW/Security/

> WWW Security Frequently Asked Questions
>
> http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html

> NIST Computer Security Resource Clearinghouse

> http://csrc.nist.gov/

Here are 18 easy tips that can go a long way towards making your NT network a safer place. This list is meant to be used only as a brief reminder - it only covers a tiny part of what you may need to think about - but it won't hurt at all to make sure you've at least considered the following items in your environment:

1. Always use NTFS disk partitions instead of FAT. NTFS offers security features, and FAT doesn't. It's that simple. If you must use a FAT partition for any reason, do not place any system files on that partition, and be careful about putting sensitive information on that FAT partition as well - you won't be able to set any access permissions for files and directories on that drive. And, if it's shared, it's open season on the shared tree.

2. Make sure that all of NT's password control features have been implemented. This includes requiring users to have strong passwords, forcing users to change their passwords at regular intervals, and hiding the last username to login (as seen in the logon dialog by default). NT can lock out accounts after so many bad password attempts. Be sure to enable this setting, as it greatly impairs an intruder's ability to brute force guess your passwords. Force the use of strong and complex passwords -- and instruct users not to write them down anywhere unless they can be safely locked up afterwards. Cryptography experts say that as long as MS doesn't change the crypto system used for the SAM database (users and passwords, et al), the best choice for passwords lengths are between 6 and 8 characters. Without going into a ton of techno babble, this causes possible time needed to crack the password to be extended considerably. And we're here to tell you, brute force guessing of passwords is one of the most popular ways of penetrating a network today. You may also want to employ the PASSFILT.DLL that comes with SP2 and SP3 - it forces strong password choices on users. Learn more about this .DLL in Microsoft's Knowledge Base article. You'll also find information in the README file accompanying the Service Packs.

3. It's no secret. The default Adminstrator account is a target for most intruders. Create a new administrator account, and take away all permissions from the existing Administrator account. Do this by creating a new user, adding them to the Administrators group, and duplicating all account policies and permissions granted to the default Adminstrator account. Once finished, go back and remove all rights and permissions from the default Administrator account. But leave it enabled, this way intruders won't know it's crippled until they take the time to actually crack the account.

4.Minimize the number of users that belong to the Administrator's group. Don't ever add someone to this group for the sake of convenience, and check it's membership routinely.

5. Enable auditing on all NT systems. Open the User Manager, and on the Policies | Audit menu, you'll find the account related events that may be audited. By using

Explorer (or File Manager) to view properties, you'll be able to establish auditing on media related objects as well.

6. Be careful about establishing NT domain trusts. Things can get out of hand quickly on larger networks with several NT domains. Microsoft has released a Domain Planning Guide that really helps a lot when designing your domain layouts, Check the MS NT web site for more information on this tool.
http:/ /www.microsoft.com/ntserver

7. Disable NetBIOS over TCP/IP network bindings where ever you can - especially on your NICs leading to the Internet, if at all possible.

8. Block all non-essential TCP/IP ports, both inbound and outbound. In particular, at least block UDP ports 137 and 138, and TCP port 139. This may prevent several types of attacks from ever making their way into your network.

9. Revoke the "Access From Network" right (using User Manager) for users that don't need to connect to that particular NT system. Those accounts can then only be used to logon on locally.

10. Periodically check your systems for unwanted user accounts. Delete or disable unused accounts. When establishing temporary accounts (for vendors, contractors, etc), be sure to set an expiration date for the account, and assign rights and permissions carefully.

11. Display a legal notice on your systems that warn each potential user that access to the system is restricted - authorized users only and sessions may be monitored. In some places its against the law to monitor computer sessions - even on your own network. With the notice, you'll most likely be able to watch an intruder if you need to, without any future legal recourse against you. Do this on your Web site, your FTP server, your NT logon screens (edit the registry), and any place else that provide a means to do so.

12. Make sure your users do not leave their NT workstations turned on and unattended. Your policies should dictate that screen savers should be activated before leaving a workstation momentarily, and users should logoff when they aren't going to return in a reasonable amount of time. Additionally, depending on your environment, you may want to have a policy mandating that systems be powered off when users leave for the day. This is a good way of helping to prevent unwanted modem dialups and rogue Web and FTP sites as well.

13. The Guest account is created by default with each NT installation. If you do not need to permit Guest users on your system, remove or disable the Guest account, and take the extra time to setup a unique user ID for each person who must access your

system temporarily. If you don't want to delete the Guest account, preferring instead to disable it, make certain you check it routinely to ensure it remains disabled.

14. Monitor your networks closely. A large percentage of break-ins occur on networks that were already secure to some extent, but simply weren't monitored closely enough. Use a robust network monitoring package to perform this task for you -- NTManage comes to mind here. You may want to use a realtime attack recognition system, like the upcoming RealSecure from ISS. And, you might want some cool registry, event log, and access control tools, like those found at Somarsoft.

15. Make sure the routers used between your untrusted bordering networks (Internet, etc) can (and are configured to) stop source routing, IP spoofing, and ICMP redirects. And it's also real good to have anti-scanning features too -- all of these items go along way towards stopping some nasty attack mechanisms.

16. Disable the Simple TCP/IP Services (if installed) using Control Panel I Services. This stops the chargen, echo, daytime, discard, and quote of the day (qotd) services. Any of which could be used for denial of service attacks. None of these services are required for proper network operation - although you should be aware that a few types of network monitors occasionally test the echo port when they cannot get a response using ping.

17. Don't run services you don't actually need - more often than not, they're neglected and frequently become the target of attack.

18. Help raise security awareness. Hey, why not start by telling a friend to come visit our site!

# *Handbook for the Computer Security Certification of Trusted Systems*

Chapter 1: Overview
Chapter 2: Development Plan
Chapter 3: Security Policy Model
Chapter 4: Descriptive Top-Level Specification
Chapter 5: Design
Chapter 6: Assurance Mappings
Chapter 7: Implementation
Chapter 8: Covert Channel Analysis
Chapter 9: Security Features Testing
Chapter 10: Penetration Testing

*NRL Technical Memorandum 5540:082A, 24 Jan 1995*

**Naval Research Laboratory, Code 5540, Washington, D.C. 203755337**

For additional copies of this report, please send e-mail to *landwehr@itd.nrl.navy.mil*, or retrieve PostScript via *http://www.itd.nrl.navy.mil/ITD/5540/publications/handbook* (e.g., using Mosaic).